REMARKS

Claim Rejections - 35 USC §102

The examiner rejected claims 1, 3, 8 and 10 under 35 USC §102(e) as anticipated by Brown et al. (5,892,826).

Regarding claim 1, the examiner asserts that Brown teaches an integrated circuit for selectively encrypting data received from a first device to send to a second device. The examiner further asserts that Brown discloses, at col. 3, lines 15-36, an encryption determination circuit having an input terminal for receiving a signal for validating the first device, and an output terminal for providing a bypass signal (verification signal) to the encryption circuitry enabling the encryption circuitry to provide encryption. The applicant respectfully disagrees.

Brown discloses a data processor (a first device) which can selectively encrypt data sent to a second device (e.g., external memory). (Col. 1, lines 53-55). Referring to FIG. 1-2, the data processor comprises a CPU core 21, an encryption determination circuit 50, and an encryption-decryption circuit 60. The encryption determination circuit 50 evaluates the internal address bus IA8-IA15 and enables the encryption-decryption circuit 60 over predetermined address ranges. This partitioning of the address space allows certain input/output peripherals or memory devices to be accessed with "cleartext" (non-encrypted) while allowing other portions (such as programs stored in external memory) to remain encrypted. (Col. 2, lines 26-42). Therefore, the encryption determination circuit 50 does not enable the encryption-decryption circuit 60 based on an authentication signal received from the CPU core 21. That is, the encryption determination circuit 50 does not first authenticate the CPU core 21 before enabling the encryption-decryption circuit 60 as recited in the claims. The encryption determination circuit 50 enables the encryption-decryption circuit 60 if the address (IA8-IA15) simply falls within a predetermined range. As such the encryption-decryption algorithm is

susceptible to a plaintext attack by modifying or replacing the CPU core 21 with an unauthenticated device. The unauthenticated device need only assert the appropriate address (IA8-IA15), present chosen plaintext data to the encryption-decryption circuit 50, and evaluate the encrypted data to decipher the encryption algorithm.

In contrast to Brown, the claim 1 recites to enable the encryption circuitry only if the device that provides the plaintext data is first authenticated. In the context of Brown, the encryption-decryption circuit 60 would not be enabled until the CPU core 21 is first authenticated. Authenticating the device which provides the plaintext data to be encrypted protects against "hackers" that would otherwise perform a chosen plaintext attack to decipher the encryption algorithm. Since Brown does not disclose or suggest to authenticate the device that provides plaintext data (the CPU core 21), the rejection should be withdrawn.

Regarding claim 3, the examiner asserts that the internal address provided by the CPU core 21 to the encryption determination circuit 50 constitutes a device identifier for identifying the CPU core 21. However, the internal address generated by the CPU core 21 is merely an address for accessing a peripheral device, such as an external memory. The address range which enables the encryption determination circuit 50 does not identify (i.e., is not unique to) the CPU core 21. Therefore any device, including unauthenticated devices, can generate the address range which enables the encryption determination circuit 50 and then perform a chosen plaintext attack to decipher the encryption algorithm. The rejection should therefore be withdrawn.

The rejection of the remaining claims should be withdrawn for the reasons set forth above.

CONCLUSION

In view of the foregoing remarks, the rejections should be withdrawn. In particular, Brown does not disclose or suggest to authenticate a device which provides plaintext data to an encryption circuit. Brown merely teaches to enable an encryption circuit based on an internal address range which could be generated by any device including an unauthentic device. Brown's encryption algorithm is therefore subject to chosen plaintext attacks. The examiner is encouraged to contact the undersigned over the telephone in order to resolve any remaining issues that may prevent the immediate allowance of the present application.

Respectfully submitted,

Date: 1/28/04 By: _____

Howard H. Sheerin
Reg. No. 37,938
Tel. No. (303) 765-1689

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on:

1/28/04 Howard H. Sheerin
(Date) (Print Name)

_____
(Signature)